REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7 May 1996	SSC Fellowship Research Paper

4. TITLE AND SUBTITLE
FUTURE WARRIORS: Special Operations Forces in the 21st Century

5. FUNDING NUMBERS

6. AUTHOR(S)
Adams, John A., Jr., LTC, USA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army War College
Root Hall, Bldg 122
Carlisle Barracks
Carlisle, PA 17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93940

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release: Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Special operations forces have played a significant role in U.S. history when waging war or conduction operations during periods other than war. As the 21st Century approaches with the advent of the high-tech battlefield, will special operations forces continue to be relevant and how will they wage information warfare? This paper examines that question by exploring the current military revolution and how it shapes the future battlefield, information warfare and its application on the future battlefield, and the role of special operations forces in conducting information warfare. The result is that special operations forces have a role to play in the future.

14. SUBJECT TERMS			15. NUMBER OF PAGES
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	**PR**	- Project
G	- Grant	**TA**	- Task
PE	- Program Element	**WU**	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

- **DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."
- **DOE** - See authorities.
- **NASA** - See Handbook NHB 2200.2.
- **NTIS** - Leave blank.

Block 12b. Distribution Code.

- **DOD** - Leave blank.
- **DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
- **NASA** - Leave blank.
- **NTIS** - Leave blank.

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

UNCLASSIFIED

USAWC STRATEGY RESEARCH PROJECT

FUTURE WARRIORS: SPECIAL OPERATIONS FORCES IN THE 21ST CENTURY

by

Lieutenant Colonel John A. Adams, Jr.
USAWC Army SSC Fellow
Naval Postgraduate School

Dr. Gordon McCormick
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

UNCLASSIFIED

ABSTRACT

AUTHOR: John A. Adams, Jr. (LTC), USA

TITLE: Future Warriors: Special Operations Forces in the 21st Century

FORMAT: Strategy Research Project

DATE: 1 June 1996 PAGES: 33 CLASSIFICATION: Unclassified

Special operations forces have played a significant role in U.S. history when waging war or conducting operations during periods other than war. As the 21st Century approaches with the advent of the high-tech battlefield, will special operations forces continue to be relevant and how will they wage information warfare? This paper examines that question by exploring the current military revolution and how it shapes the future battlefield, information warfare and its application on the future battlefield, and the role of special operations forces in conducting information warfare. The result is that special operation forces have a role to play in the future.

INTRODUCTION

Then I heard the voice of the Lord saying, "Whom shall I send? And who will go for us?"
And I said, "Here am I. Send me!"

Isaiah 6:8[1]

This verse of Old Testament Scripture portrays the commissioning of Isaiah as he eagerly answered God's call. This same scripture is posted throughout the Special Operations (SO) community and has come to symbolize the willingness of the special operations trooper to answer the beating of our nation's war tocsin when it has sounded in past and present wars. When it sounds in the next century, will special operations forces (SOF) still answer the call? Will they be prepared to answer the call when it pertains to waging information warfare? How might special operations forces be employed in an information-based campaign?

Before we can usefully speculate on the future role of special operations forces, we must ask ourselves the following question: What will the future battlefield look like? That question continues to haunt a myriad of military strategists, who currently believe that we have entered a revolution in military affairs. With the sophistication of our current weapon systems, the infusion of emerging technology, and the reliance on computer systems, we now find ourselves fighting something called information warfare.

Will special operations forces have a role to play in a future "information war?"

This paper will examine that question by addressing the following issues:

- the current revolution in military affairs (RMA) and how it shapes the future battlefield.
- information warfare and its application on the future battlefield.
- the organization of modern military "systems" and how information warfare is to be used against them.
- special operations forces and how they are to be used in waging information warfare.

This paper will argue that special operations forces are warriors for the future, capable of waging information warfare on the battlefield of the future. When the call to war sounds in the next century, special operations forces will once again answer the call, physically fit, mentally prepared, and technically proficient.

THE BATTLEFIELD IN THE NEXT CENTURY

Are we in the middle of a revolution in military affairs, commonly referred to as the RMA? One could very easily come to that conclusion based on the outcome of Operation DESERT STORM, with its short duration, reduced casualties, and the emergence of sophisticated command and control and weapons systems. But is it truly a revolution? We see that a revolution is occurring throughout the information technology field around the world, and in all "likelihood these technologies will continue such growth patterns for at least two more decades."[2] With the rate of advance in technology increasing exponentially on a daily basis, more precise and lethal weapon systems are just around the corner. These systems, "when coupled with continuing improvements in sensors and information processing," will be used "by military planners as they define the future battlefield."[3] General Sullivan, former Chief of Staff of the Army, further identifies "five trends" which "will define the operational environment," and they are as follows:

- Greater lethality and dispersion.
- Increased volume and precision of fire.
- Better integrative technology leading to increased efficiency and effectiveness.

- Increasing ability of smaller units to create decisive results.
- greater invisibility and increased detectability.[4]

The United States must take advantage of these technological advances as it responds to future wars and conflicts, as we know our adversaries will. We must also respond doctrinally to these changes with regard to how the future army, Force XXI, shapes up. As Metz and Kievit point out, "This fusion is expected to allow smaller military forces to produce rapid, decisive results through synchronized, near-simultaneous operations throughout the breadth and depth of a theater of war."[5]

The implications and possible impacts of the revolution in military affairs are important to both conventional and special operations forces alike. Although most thinking about the revolution is focused on conventional, combined-arms warfare, the technology, the organization, and the techniques spawned by the RMA also apply to conflict short of war.[6] In fighting conventional wars, we will see battlefields far larger than in the past, some exceeding 200 miles square. And they will be fought at a tempo much quicker than DESERT STORM, in all types of light and weather conditions and concluding them in days or weeks.[7] The objective of these type of wars would be "to wield military power across space

and through time with heretofore unimaginable precision and accuracy."[8]

It is more likely that we will see conflict short of war, a role readily adaptable to special operations forces. Since the end of World War II, more than 160 low-intensity conflicts, most being wars of national liberation, have been waged throughout the world.[9] We will also see additional fracturization of "failed states" and the rise of associations and federations of new terrorists, narcotraffickers, and other guerilla groups as they learn to "master modern technology".[10] Will we fight these battles with the same tactics? As Brian Nichiporuk and Carl Builder point out:

> Most potential U.S. opponents around the world now realize that it would be futile to challenge the American military with regular forces on a conventional battlefield, and if they haven't already, they will most certainly devise plans for matching their particular areas of strengths against areas of perceived U.S. weaknesses-as they may have perceived it in Bosnia or Somalia. Opponents who have unorthodox doctrines or unconventional objectives will be more difficult to deal with than adversaries who operate in a conventional Western military mindset.[11]

Regardless of the type of conflict that lies ahead, the microchip has revolutionized "the way that we are likely to fight our future wars."[12] And as a result, we must accept the fact that the Information Age has arrived and turn our attention to waging information warfare.

INFORMATION WARFARE

What is information warfare? In the broadest sense, information warfare is "simply the use of information to achieve our national objectives."[13] At the other end of spectrum, we find, however, that we must "resist the tendencies still found in some circles to reduce information warfare to meaning little more than computer warfare and cyberspace security."[14] To balance out the playing field, the Department of Defense's Director of Information Warfare views information warfare as

> ....actions taken to achieve information superiority in support of national military strategy by affecting adversary information systems while leveraging and protecting our own information and information systems. IW is an overarching, integrating strategy to recognize the importance and utility of information in the command, control and execution of military forces and in the implementation of national policy. IW addresses the opportunities and vulnerabilities inherent in increasing dependency on information and the use of information throughout the conflict spectrum. It focuses on information systems (including associated transfer links, processing nodes and the systems' human factors) and the information technology inherent in weapons systems. IW has offensive and defensive elements, but begins with intentionally designing and developing our Command, Control, Communications, Computers and Intelligence (C4I) architecture to provide decision maker distinct information superiority throughout the conflict spectrum.[15]

But how is information warfare reduced to layman's terms? It is simply a study of man, the way man thinks, and the process man

goes thorough in making decisions. Information warfare is about influencing that decision-making process to achieve one's goals.[16] In order to make decisions, man must have information. And when waging war man must, first, have the information he requires to will tip the balance of power in his favor, particularly if he is outnumbered or outgunned. At the same time, he must prevent his adversary from knowing too much about himself.[17] The purpose of information warfare, therefore, is "to control, manipulate, deny information, influence decisions, and degrade or ultimately destroy adversary systems while guarding friendly systems against such action."[18]

Now, because more countries are becoming sophisticated in information technology and the world is becoming more linked together by networks, this type of warfare is applicable to future wars and operations other than war. In much the same manner as achieving air superiority over an opponent, a country expands its ability to dominate that opponent by achieving information superiority. By doing so, a multitude of new options may be applied to the traditional modes of waging war.

The advantages of waging this style of warfare are numerous. First, it may prevent the outbreak of war. Second, it allows the concentration of our superior technology to focus on the whole

adversarial military system across all levels of war. Third, a demoralizing effect may be achieved, after hostilities have been initiated, which would cause the adversary to withdraw from the battlefield. Fourth, information warfare is selective. And lastly, because technology can be a force multiplier, engagement forces may be reduced in size.

War is waged in order to impose one's will over an adversary, with the objective being to not become decisively engaged. As Sun Tzu noted, "....those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations."[19] Implementing an information warfare campaign may resolve the situation prior to the initiation of hostilities. Denying an opponent the ability to observe the battlefield or deceiving him by distorting his perception of what is actually on the battlefield or even where the battlefield is located may paralyze his decision-making process sufficiently to preclude his ability to wage war.

Secondly, information warfare allows the integration of U.S. superior technology "in a way resembling the effects of a single weapon" across all levels of war. Technology in "the Information Age" is moving in the direction that will allow us to simultaneously strike the enemy across all levels of war and

"throughout the breadth and depth of the operational area." Upon receiving such a shocking blow, the enemy yields the initiative and loses his flexibility to have any impact on the battlefield. The results are "the total collapse of resistance" with a "minimum loss of life" on all sides and reduced "destruction of resources and infrastructure."[20]

A third advantage to conducting information warfare is the ability to demoralize an adversary's forces and/or political system through an effective propaganda campaign or create within his forces the perception of impending annihilation in such a way as to stop them from fighting.[21] Martin Libicki points out that psychological operations "encompasses the use of information against the human mind."[22] Both the North Vietnamese and Somalis used effective propaganda against the United States in driving us from the battlefield. Daniel Magsig points out that

> Aideed's ultimate success was in using this strategy to set up an ambush of U.S. troops which was naturally televised via CNN into every American home. This psychological information warfare operation, which included televised images of dead Americans being dragged through the streets, succeeded in eliminating most public support for U.S. involvement in Somalia, and very soon afterwards, the U.S. pulled out.[23]

Fourth, information warfare is selective, which means it can be applied to parts of a system vice the whole system. As such, it can be directed against any portion of a society, which "includes

military, technological, economic, political, social, and ideological/religious issues."[24] If the military establishment is the target, information warfare may be judiciously applied to "any one of the steps" of an adversary's decision making loop or his "ability to move from one step to the next" as "an example of attacking the interconnections between systemic elements."[25] In speaking about Operation DESERT STORM, Alvin Toffler

> points out that the earliest attacks targeted "microwave relay towers, telephone exchanges switching rooms, fiber optic nodes, and bridges that carried coaxial communications cables." This had the effect of either silencing them, or forcing "the Iraqi leadership to use backup systems vulnerable to eavesdropping that produced valuable intelligence." These attacks were coupled with direct strikes at Saddam's military and political command centers themselves, designed to destroy or isolate the Iraqi leadership and cut off it off from its troops in the field. The task, put differently, was to disrupt the brain and nervous system of the Iraqi military. If any part of the war was "surgical," it was, so to speak, brain surgery.[26]

The last advantage of conducting information warfare is the reduction of forces necessary to wage war. Advanced technologies can be expected to provide the United States with an effective force multiplier "that will allow U.S. forces to achieve more while making do with less."[27] The possibility then exists that current unit configuration may be redesigned, allowing for "smaller force packages,"[28] to take advantage of the advent of these more lethal weapon systems or get "more bang for the buck."[29]

MILITARY SYSTEMS

Now that we know what information warfare is, how then do we apply it? To do that, we must briefly examine the nature of military organizations. A military organization, like any other form of organization, might be defined generally as a system of interdependent and interacting elements designed to achieve a common goal. To borrow from the work of W. Richard Scott, they are also characterized by "fixed boundaries, a normative order, authority ranks, a communications system, and an incentive system."[30] The synergistic interaction of a military organization's constituent elements is designed to achieve an effect that is greater than the sum of its parts. Such an organization, operating as a synchronized system in other words, can be expected to generate an outcome that simply could not be achieved in the absence of effective internal coordination, even with the same level of effort.

Systems or organizations can either be loosely or tightly coupled. Loosely coupled systems have fairly loose connections between the various elements that make up the system. The organization's constituent elements, in such a case, are relatively autonomous. Although decisions may be made centrally, execution of

those decisions will be decentralized. For reasons of security, underground organizations are frequently structured in a loosely coupled manner. Tightly coupled systems, by contrast, are closely networked together. An example of this system would be any modern day army.

Organizations can also be defined by their degree of complexity.[31] Complexity, in turn, is defined by the number of subunits within the organization, how these subunits are arranged, and the command and control required in dealing with the different parts. Obviously, an organization becomes more complex when it grows in size, either horizontally or vertically. If the organization grows horizontally, power will remain centralized "with the top management retaining most of the control." With vertical growth, however, "lower-level personnel are allowed to make more of the decisions."[32] All things being equal, an organization's command and control requirement is directly related to its level of complexity and its degree of coupling.

Formalization describes how rules and/or procedures and power is used within an organization. Rules and procedures differ within organizations from very lax to extremely rigid. The method by which power is distributed within an organization "has major consequences for the performance of an organization and the

behavior of its members."[33] Tightly controlled organizations are very rigid structures where members exhibit little initiative and would be easier to attack and bring down. Loosely controlled organizations are just the opposite. Because of decentralized power, each echelon has initiative to take action which would make it harder to attack the organization as a whole.

Elements within an organization are linked together in a systemic manner with a communication system that transmits and receives information. This system and the information that flows through it, by definition, is what makes the difference between a disassociated collection of individual elements, and a military organization that is capable of operating in a collective, coordinated manner. As Richard Hall notes in his book,

> Communications is most important, therefore, in organizations and organization segments that must deal with uncertainty, are complex, and have a technology that does not permit easy routinization.[34]

Looking at today's modern military system, we see that they are more tightly coupled, as well as more complex in nature. All things being equal, tight coupling and complexity are sources of opportunity and sources of risk when analyzing the system as a target. They are sources of organizational control and efficiency on one hand, and they are a potential source of vulnerability on the other. In the latter case, disruptions anywhere in a highly

complex and tightly coupled system will be felt throughout the system as a whole. This is a potential vulnerability. Loosely coupled systems may also be exploited, but in a more systematic manner.

APPLICATION OF INFORMATION WARFARE

The objective of information warfare is to paralyze the enemy by attacking the information links that tie his military system together. This might be equated with attacking the enemy's nervous system. Successfully neutralizing the enemy's nervous system can be a decisive and potentially cost effective way of neutralizing the enemy. Currently, successful conventional battle is characterized by high enemy casualties and a low prisoner of war count, commonly referred to as a war of attrition. However, a successful information war would be characterized by low casualties and a high prisoner of war count.

Operations have been conducted against information targets in the past. To some degree, these have contributed to the success of a conventional campaign. As a general rule, however, our approach to operations conducted to sever information ties or communication links has been disjointed. Even where they contributed to the

success, they have served to support rather than substitute for conventional attacks. In information war the opposite would be true. Information operations will be the primary missions conducted in a campaign plan, and conventional operations would be reduced to supporting them.

In the end, however, a true information warfare campaign is a complex problem requiring an integrated or joint solution. Every service and special operations force will have something to contribute. Any special operations force contribution must be carefully integrated with the efforts of other branches to develop a comprehensive solution. It must be thought of as a campaign in the truest sense.

The problem must also be approached dynamically, rather than statically. Not everything will be known about an enemy's information system to effectively target it prior to the beginning of the war, nor will it be possible to effectively target everything that is known about his system. One reason why everything will not be known about the enemy's information net is that it will not totally reveal itself prior to our initial success in taking it down. We may not know, for example, how fast, or to what degree the enemy will reconstitute his information net after it has been damaged in the opening engagements of the campaign. He

may not know himself until called upon to do so. We must, as quickly as possible, follow the wartime evolution of his information net to continue to bring it down over time until it reaches the point of total failure. Consequently, we must approach the problem in an iterative manner. During the opening period of the war, our objective should be to paralyze the enemy's information net in a series of rapid steps. This will go on until this system has been compressed to such a degree that the system as a whole experiences catastrophic collapse.

We accomplish our objectives by destroying or disabling the information system that ties our adversary"s larger system together as an organization. As long as this information net is intact, the enemy is in position to do battle. His military system is able to operate in a manner that is greater than the sum of its parts. Once his net is destroyed or compressed to such a degree that it collapses, his military system will disintegrate. It will devolve to its constituent elements to become something that is less than its sum. Each element can then be systematically addressed at leisure.

DEFINING SPECIAL OPERATIONS

What are special operations and special operations forces and how are they to be used in waging information warfare? Special operations, according to JCS Pub 1-02, are defined as:

> operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or psychological objectives by unconventional military means in hostile, denied, or politically sensitive areas. These operations are conducted during peacetime competition, conflict, and war, independently or in coordination with operations of conventional, nonspecial operations forces. Political-military considerations frequently shape special operations, requiring clandestine, covert, or low visibility techniques and oversight at the national level. Special operations differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets. Also called SO.[35]

As defined, special operations are conducted across the range of military operations in war and operations other than war. While special operations are described by such characteristics as "simplicity, enhanced by innovation, imagination, and subtlety,"[36] these terms can also be used to describe conventional military operations. Special operations can be distinguished from conventional operations by the following five requirements: "unconventional training and equipment, political sensitivity,

unorthodox approaches, limited opportunity, and need for specialized intelligence."[37]

Special operations forces are "those active and reserve component forces of the military Services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations."[38] From austere beginnings in 1952, post World War II special operations forces were developed with an initial mission to train and "lead guerrilla units behind the Iron Curtain in case of war with the Soviet Union." That role was expanded "to counterinsurgency" in the 1960's in a theater of conflict half a world away.[39] Special operations forces have evolved over time from many "historical experiences" around the world. Additionally, with the passage of the Goldwater-Nichols Act in 1986, "Congressional legislation and the evolving security environment" has expanded the mission requirements for the special operations forces community. As outlined the USSOCOM Pub 1,

> the principal special operations missions are: direct action (DA), special reconnaissance (SR), foreign internal defense (FID), unconventional warfare (UW), combating terrorism (CBT), counterproliferation (CP), civil affairs (CA), psychological operations (PSYOP), and information warfare (IW)/command and control warfare (C^2W).[40]

To conduct these missions requires people with "special skills and special characteristics-aggressiveness, initiative, mature

judgment, and an attitude that inspires respect in friend and foe alike." These "high caliber professionals" from the different Services undergo a selection process to gain admittance to the various service-specific special operations units. Once inducted, these service members begin an intensive training regimen, honing the skills necessary to conduct the above listed missions. Additional training conducted "with conventional forces" and "other SOF components" enables "all SOF personnel to function effectively as members of a close-knit, self-contained team."[41]

Despite the drawdown within the Armed Forces as a whole, the operations tempo has increased, particularly for special operations forces. Between the years 1991-1994, deployment of special operations forces elements increased by 125% with "more that 43,900 special operations soldiers, sailors, and airmen" being "sent to more than 140 countries to accomplish some 1,300 missions ranging from humanitarian relief to combat operations." Yet there has been no "increase in force size" within the special operations forces corresponding to this "dramatic increase in the OPTEMPO."[42]

These figures illustrate the importance special operations forces play in accomplishing U.S. policy in the various geographical hot spots of the world. As General Shelton points out in his confirmation hearing:

> SOF serve three strategic purposes in the promotion of national security: (1) SOF expand the range of options available to decision-makers confronting an increasing number of military operations that fall between wholly diplomatic initiatives and overt use of large conventional forces, such as terrorism, insurgency, narcotics trafficking, subversion, and sabotage. (2) SOF provide a strategic economy of force and generate a strategic advantage disproportionate to the resources they represent. They are able to operate without the infrastructure often needed by a larger force. SOF can be skillfully integrated with conventional forces as a force multiplier, increasing the efficiency and effectiveness of the total military effort. (3) SOF provide the broadest range of capabilities to react to situations requiring exceptional sensitivity, such as benign, noncombatant humanitarian assistance and peace operations missions.[43]

SPECIAL OPERATIONS MOVES INTO THE 21ST CENTURY

As shown above, special operations forces have changed to meet each new threat throughout their brief history. As the world changes around us with the rising of each new dawn, how then do we shape special operations forces for its role in waging information warfare? Is change needed to the way SOF operations are currently being conducted?

"As the world situation changes," each mission will be evaluated for relevancy "to see if they fit within the definition of special operations."[44] In the near term, special operations forces missions will not change. Changes will occur in other areas. One change is the type of targets that must be observed or

engaged. This will occur during war or operations other than war or against tightly or loosely coupled systems. Direct action and special reconnaissance missions might be carried out against "stock exchanges, or utility grids, or telephone networks, or all of the above, as well as purely military targets."[45] A second change will be in technology. The technological improvements, such as "extremely lethal, usually standoff, precision-strike weapons systems and automation-assisted systems of command, control, and communications,"[46] will improve special operations forces's ability to move, shoot, and communicate in executing all current roles and missions. The last change will be in how the missions are tasked. In executing the campaign plan, a more concerted effort should be made to task the right unit with the right target, similar to the daily air tasking letter. The missions will be executed independently, yet are tied to the bigger picture. Therefore, special operations forces, by remaining flexible, will be in a position to support all future campaigns.

However, "as computers become weapons" and the future battlefield becomes more technologically advanced, special operations forces must become increasingly able to enlist these weapons to support their objectives. Most potential target groups, from narcotraffickers to African warlords, are becoming more

dependent "on radios, cellular telephones, fax machines, and computers, all of which are vulnerable to electronic intelligence-gathering and disruption."[47] As a result, Kievet and Metz further contend that

> missions such as foreign internal defense could undergo substantial transformation: Instead of training friendly forces in basic military skills, Special Forces would train them in information warfare. The laptop computer, rather that the AK-47, M-16 or RPG, could become the first-line weapon for both insurgents and counterinsurgents. Special Forces would have to develop methods for teaching information warfare across cultural obstacles just as they currently do to bridge those obstacles in teaching basic military skills.[48]

Additionally, direct action missions would take on a new dimension involving computer related operations. Instead of destroying a telephone-switching station to knock out a grid of phone lines, "a computer virus" can be "inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system." Psychological operations would be a major player in implementing the campaign plan. An example of operations would be to misdirect enemy forces by flooding their radio communications with false commands and misdirections. Another would be to "jam the enemy's TV broadcasts with propaganda messages that turn the populace against its ruler." The intent of these operations is "to launch rapid, stealthy, widespread and

devastating attacks on the military and civilian infrastructure of an enemy."[49]

The battlefield has gone high tech. And as a result, these technological advances must be exploited. Special operations forces are versatile enough to handle these changes and flexible enough to remain mission focused. Today's commanders, however, must ensure that the future special operations operator is provided with the training and education to meet the challenge.

CONCLUSIONS AND RECOMMENDATIONS

> Colonel Yasotay, an officer in Genghis Khan's army, is said to have told his general, "when the hour of crisis comes, remember that 40 selected men can shake the world." The colonel, of course, was not referring to the existence of godlike figures from Roman or Greek mythology, or a band of superwarriors capable of single-handedly destroying whole armies and conquering entire nations. The point here is more subtle and complex: When undertaking missions of importance to the state or a military campaign, a small and audacious force of skilled warriors has the capacity to influence events far beyond any physical measure of their capability.[50]

The past chronicles of special operations forces reveals that they have successfully accomplished a wide range of missions when called upon to do so. Flexibility, versatility, and quality people have been the hallmarks of character that have allowed special operations forces to be successful. These same characteristics

will allow special operations forces to move into the 21st Century and adapt to the future battlefield. That future battlefield must be assessed now to determine the trends which affect special operations forces "in order to ensure enduring relevance of their capabilities."[51]

ENDNOTES

1. The Holy Bible, New International Version (Colorado: International Bible Society, 1973), 600.

2.Brian Nichiporuk and Carl H. Builder, Information Technologies and the Future of Land Warfare (Santa Monica: Rand, 1995), 7-8.

3.Ibid., 48.

4.Gordon R. Sullivan and Anthony M. Coroalles, The Army in the Information Age (Carlisle Barracks: Strategic Studies Institute, 31 March 1995), 3-4.

5.Steven Metz and James Kievit, "The Siren Song of Technology and Conflict Short of War," Special Warfare 9, no. 1 (January 1996): 2.

6.Ibid.

7.Art Pine, "Military Nears Revolution in Weapons, War Strategy," Los Angeles Times, 20 March 1996, p. 1.

8.Sullivan and Coroalles, The Army in the Information Age, 7.

9.Martin van Crevald, The Transformation of War (New York: The Free Press, 1991), 20.

10.Steven Metz and James Kievet, The Revolution in Military Affairs and Conflict Short of War (Carlisle Barracks: Strategic Studies Institute, 25 July 1994), 4.

11.Nichiporuk and Builder, Information Technologies and the Future of Land Warfare, 49.

12.Sullivan and Coroalles, The Army in the Information Age, 2.

13.George J. Stein, "Information Warfare," Airpower Journal IX, no. 1 (Spring 1995): 32.

14.John Arquilla and David Ronfeldt, "Book Reviews," Comparative Strategy 14, no. 3 (July-September 1995): 337.

15.Richard Power, "Information Warfare," Netscape. URL:http://www.digpath.com/news/10_13_95/1tech003.html.

16.Stein, "Information Warfare," Airpower Journal, 32.

17.Alvin and Heidi Toffler, War and Anti-war (New York: Little, Brown and Company, 1993), 141.

18.Robert Garigue, "Information Warfare," Netscape. FTP://ftp.cse.dnd.ca/pub/formis/iw/iw_dver2.ans.

19.Samuel B. Griffith, Sun Tzu The Art of War, (New York: Oxford University Press, 1963), 79.

20.Sullivan and Coroalles, The Army in the Information Age, 7-13.

21.Richard Szafranski, "A Theory of Information Warfare," Netscape. URL:http://www.cdsar.af.mil/apj/szfran.html.

22.Martin Libicki, What is Information Warfare (Washington: National Defense University, August 1995), 13.

23.Daniel Magsig, "Information Warfare," Netscape. URL:http://www.sease.gwu.edu/student/dmagsig/infowar.html.

24.Ibid.

25.Ibid.

26.Toffler, War and Anti-war, 71.

27.John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review 22, no. 3 (Summer 1994): 24.

28.Donald E. Ryan, Jr., "Implications of Information-Based Warfare," Joint Force Quarterly, no. 6 (Autumn/Winter 1994-95): 116.

29.Toffler, War and Anti-war, 76.

30.Richard H. Hall, Organizations Structure and Process (Englewood Cliffs: Prentice-Hall, Inc., 1972, 8.

31.Ibid., 140.

32.Ibid., 156.

33.Ibid., 177.

34.Ibid., 271.

35.Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington: Joint Chiefs of Staff, 23 March 1994), 353.

36.Frank R. Barnett, B. Hugh Tovar and Richard H. Shultz, eds., Special Operations in US Strategy (Washington: National Defense University Press, 1984), 35.

37.H. Allen Holmes and Wayne A. Downing, United States Special Operations Forces: Posture Statement (Washington: U.S. Special Operations Command, 1994), 3-4.

38.Joint Pub 1-02, 353.

39.Eliot A. Cohen, Commandos and Politicans (Boston: Harvard University, 1978), 25.

40.U.S. Special Operations Command, Special Operations in Peace and War, USSOCOM Pub 1 (Tampa: USSOCOM, 25 January 1996), 3-1-3-4.

41.Holmes and Downing, 7.

42.CINCSOC Nominee LTG Henry Shelton, Testimony before Senate Armed Services Committee, 1 February 1996, Washington, D.C.

43.Ibid.

44.USSOCOM Pub 1, 3-2.

45."The Information Advantage," The Economist (10 June 1995): 19.

46.Metz and Kievit, Special Warfare, 2.

47.Ibid., 2-9.

48.Ibid., 9.

49.Douglas Waller, "Onward Cyber Soldiers," Time 146, no.8 (21 August 1995): 38.

50.Steven Lambakis, "Forty Selected Men Can Shake the World: The Contributions of Special Operations to Victory," Comparative Strategy 13, no. 2 (April-June 1994): 211.

51.H. Allen Holmes, "State of Special Operations," Defense Issues 9, no. 87 (15 November 1994): 1.

BIBLIOGRAPHY

Anthes, Gary. "Info Warfare Risk Growing." Computerworld 29, no. 21 (22 May 1995): 1,16.

Arquilla, John. "The Strategic Implications of Information Dominance." Strategic Review 22, no. 3 (Summer 1994): 24-30.

Arquilla, John, and David Ronfeldt. "Book Reviews." Comparative Strategy 14, no. 3 (July-September 1995): 331-341.

_____. "Cyberwar is Coming!" Comparative Strategy 12, no.2 (April-June 1993): 145-169.

Barnett, Frank R., B. Hugh Tovar, and Richard H. Shultz, eds. Special Operations in U.S. Strategy. Washington: National Defense University Press, 1984.

Cohen, Eliot A. Commandos and Politicans. Boston: Harvard University, 1978.

Cohen, Frederick B. "Comment on Special Report on Information Warfare." Netscape. URL:http://www.all.net/journal/letters//iwar.html.

Collins, John M. America's Small Wars: Lessons for the Future. Washington: Brassey's, 1991.

_____. Special Operations Forces. Washington: National Defense University Press, April 1994.

De Landa, Manuel. War in the Age of Intelligent Machines. New York: Zone Books, 1991.

Downing, Wayne A. "Special Operations Forces Evolve, Adapt to Change." Defense Issues 9, no. 14 (1994): 1-7.

Garigue, Robert. "Information Warfare." Netscape. FTP://ftp.cse.dnd.ca/pub/formis/iw/iw_dver2.ans.

Goodman, Glenn W., Jr. "SOCOM: Defining Its Equipment Priorities." Armed Forces Journal International 132, no. 2 (September 1994): 61.

_____. "Warrior-Diplomats - Not Political Warriors: Sound Guidelines for Employing US Special Operations Forces." Armed Forces Journal International 132, no. 7 (February 1995): 42.

Griffith, Samuel B. Sun Tzu The Art of War. New York: Oxford University Press, 1963.

Grimes, Vincent P. "Global Disarray Demands Special Operations Force." National Defense 79, (December 1994): 44-45.

Hall, Richard H. Organizations Structure and Process. Englewood Cliffs: Prentice-Hall, Inc., 1972.

Holmes, H. Allen. "State of Special Operations." Defense Issues 9, no. 87 (15 November 1994): 1-4.

Holmes, H. Allen, and Wayne A. Downing. United States Special Operations Forces: Posture Statement. Washington: U.S. Special Operations Command, 1994.

The Holy Bible. New International Version. Colorado: International Bible Society, 1973.

"The Information Advantage." The Economist 335, no. 7918 (10 June 1995): 5-20.

Jeremiah, David E. "Melding Special Operations with Forces of the Future." Defense Issues 7, no. 7 (1992): 1-4.

Joint Chiefs of Staff. DoD Dictionary of Military and Associated Terms. Joint Pub 1-02. Washington: Joint Chiefs of Staff, 23 March 1994.

_____. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Joint Pub 6-0. Washington: Joint Chiefs of Staff, 30 May 1995.

Lamb, Christopher. "Perspectives on Emerging SOF Roles and Missions." Special Warfare 8, no. 3 (July 1995): 2-9.

Lambakis, Steven. "Forty Selected Men Can Shake the World: The Contributions of Special Operations to Victory." Comparative Strategy 13, no. 2 (April-June 1994): 211-221.

Libicki, Martin C. What is Information Warfare. Washington: National Defense University Press, August 1995.

Locher, James R., III. "Focusing on the Future: The Role of SOF in Emerging Defense Strategy." Defense Issues 5, no. 5 (March 1992): 10-13.

Magsig, Daniel. "Information Warfare." Netscape (7 Dec 1995). URL:http//www.seas.gwu.edu/student/dmagsig/infowar.html.

McRaven, William H. Special Operations. Novato, CA: Presidio Press, 1995.

Metz, Steven, and James Kievet. The Revolution in Military Affairs and Conflict Short of War. Carlisle Barracks: Strategic Studies Institute, 25 July 1994.

_____. "The Siren Song of Technology and Conflict Short of War." Special Warfare 9, no. 1 (January 1996): 1-9.

_____. Strategy and the Revolution in Military Affairs: From Theory to Policy. Carlisle Barracks: Strategic Studies Institute, 27 June 1995.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." Netscape. URL:http://www.rand.org/publications/MR/MR661/MR661.html.

Nichiporuk, Brian and Carl H. Builder. Information Technologies and the Future of Land Warfare. Santa Monica, CA: RAND, 1995.

Pine, Art. "Military Nears Revolution in Weapons, War Strategy." Los Angeles Times (Washington Edition), 20 March 1996, p. 1.

Power, Richard. "Information Warfare." Netscape. URL:http://www.digpath.com/news/10_13_95/1tech003.html.

Ryan, Donald E., Jr. "Implications of Information-Based Warfare." Joint Force Quarterly, no. 6 (Autumn/Winter 1994-95): 114-116.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunders Mouth Press, 1994.

Scott, James T. "Special Operations Forces: Facing Change and Challenge." Army 45, (April 1995): 20-24.

_____. "U.S. Special Operations Command: Meeting Tomorrow's Challenges Today." Army 44, (October 1994): 165-171.

Shelton, Henry, CINCSOC Nominee. Testimony before the Senate Armed Services Committee, 1 February 1996, Washington, D.C.

Stein, George J. "Information Warfare." Airpower Journal 9, no. 1 (Spring 1995): 30-39.

Stiner, Carl W. "Strategic Employment of Special Operations Forces." Military Review, (June 1991): 2-13.

_____. "US Special Operations Forces: A Strategic Perspective." Parameters 22, (Summer 1992): 2-13.

Sturgill, Claude C. Low-Intensity Conflict in American History. Westport, CT: Praeger, 1993.

Sullivan, Gordon R., And Anthony M. Coroalles. The Army in the Information Age. Carlisle Barracks: Strategic Studies Institute, 31 March 1995.

Szafranski, Richard. "The Theory of Information Warfare." Netscape. URL:http://www.cdsar.af.mil/apj/szfran.html.

Toffler, Alvin and Heidi. War and Anti-war. New York: Little, Brown and Company, 1993.

U.S. Special Operations Command. Special Operations in Peace and War. USSOCOM Pub 1. Tampa: USSOCOM, 25 January 1996.

Van Creveld, Martin. The Transformation of War. New York: The Free Press, 1991.

Waller, Douglas C. The Commandos: The Making of America's Secret Soldiers. New York: Simon & Schuster, 1994.

_____. "Onward Cyber Soldiers." Time 146, no. 8 (21 August 1995): 38-44.

Waltz, Kenneth N. Theory of International Politics. New York: McGraw-Hill, 1979.

White, Terry. Swords of Lightning: Special Forces and the Changing Face of Warfare. Washington: Brassey's, 1992.

Yarborough, William P. "Emerging SOF Roles and Missions: A Different Perspective." Special Warfare 8, no. 3 (July 1995): 10-12.